Policy: 8010-2- Computer Information Systems Policy
Section: Computer Information Systems
Office/Department: Office of IT Infrastructure

Reports To: Division of Information Technology
Contact: 404-631-1000

Introduction

Information is essential to the Department of Transportation (DOT) in conducting the business mandated to it by law. This information, both in paper and electronic form, is valuable and can be sensitive regarding personal privacy and intellectual property rights.

DOT utilizes this information to a large degree with computer information systems and networks. DOT has made a substantial investment in human and financial resources to create its electronic infrastructure that is an integral part of daily business functions.

A Computer Information Systems Policy has been established in order to:

- Comply with Federal and state laws and regulations regarding information security.
- Safeguard the systems and information contained within these systems.
- Reduce business and legal risk.

The policy applies to employees, contractors, consultants, temporaries, and other workers (hereafter collectively referred to as users) at all facilities of the Department of Transportation, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by DOT or is connected to the Department's network.

Policy

Access to the Intranet and Internet is available to users whose duties require them to conduct DOT business. Proper use of the Intranet and Internet at work is the employee's responsibility. Occasional use of GDOT Intranet and Internet for non-work related reasons is permitted so long as it doesn't involve inappropriate use as described in existing policies 8010-3, 8005-1, and 8010-2. Any such use should be brief, infrequent, and shall not interfere with User's performance, duties and responsibilities. All activity is monitored and subject to review at any time. This privilege may, however, be withdrawn if abused.

While the Department administration desires to provide a reasonable level of privacy, users should be aware that anything created and/or stored on the Department's systems is the property of DOT. Anyone using DOT's electronic infrastructure shall have no expectation of privacy.

Normal network access will utilize DOT provided equipment and network connections. However, some situations may arise requiring the use of non-Department equipment or access. This must be approved by the Office Head, District Engineer or Division Director prior to the initial access and must meet security requirements specified by the Division of Information Technology (IT). These security requirements include, but are not limited to:

1. Continual execution of an approved virus-scanning software with a current virus database on all computers connected to the DOT network.
2. The installation and use of firewalls on the non-Department equipment

To assure compliance with Federal and state laws and to protect DOT's infrastructure, management reserves the right to access and review anything created and/or stored on DOT systems. This could include anything stored on the user's assigned DOT computer's hard drive. Authorized individuals within DOT will conduct random reviews of all traffic across DOT systems, as well as information contained thereon, including, but not limited to, email and internet usage, by using direct access and/or archival data to detect the abuse or misuse of these resources. Deletion from a user's file does not constitute deletion from the archived files. These reviews can be done with or without notice to the user. To reduce the possibility of compromise to DOT's infrastructure, the installation and/or running of hardware and/or software on the Department's infrastructure that is not specifically authorized by IT is prohibited.

To assure compliance with the U.S. Copyright Law, copyright and license agreements must not be violated. Users who utilize the Department's electronic infrastructure should familiarize themselves with the requirements of the User Responsibilities and Acknowledgments to the Computer Information Systems Policy, 8010-3. Users must acknowledge their understanding and agreement to policy requirements by signing the Computer Information Systems Policy User Responsibility Agreement form, DOT 1801.

Violations

Employees who violate the Computer Information Systems Policy will be subject to appropriate disciplinary action up to and including termination of employment. Other than employees, users that violate the Computer Information Systems Policy will be subject to losing access to the Department's electronic infrastructure.

Possible violations of Federal or state law will be referred to law enforcement authorities for further investigation.

RELATED INFORMATION

The User Responsibilities and Acknowledgments to the Computer Information Systems Policy, 8010-3, and the Computer Information Systems Policy User Responsibility Agreement form, DOT 1801may be read in the Computer Information Section of Publications.

References:

User Responsibilities and Acknowledgments to the Computer Information Systems Policy, 8010-3
Computer Information Systems Policy User Responsibility Agreement form, DOT 1801

History:

annual review: 10/30/14;
added to TOPPS: 11/21/02
Reviewed: 10/30/2014